International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 4, April - 2014

Scrutiny of the Indian attempt to Internet Voting

The beginning of e-voting in India

Aparna Khare
Department of IT and Electronics,
National Informatics Centre,
Government of India
Lucknow,
Uttar Pradesh, India.

***Abstract*-With e-governance turning up as the one of the top initiatives for a better government in the recent times in India, the idea of internet voting, also known as online voting or e-voting or i-voting has become the next big challenge to get to grips with. Worldwide, efforts are being made, small scale as well large scale to take the most fundamental right of a citizen to the next level of convenience, online voting. This paper briefly pinpoints the advantages and challenges of internet voting, a summarized account of the attempts and successes made worldwide for achieving it followed by a review of the attempt of an Indian state to put forth the first steps in the direction of turning this idea into a tangible reality.**

Keywords- internet voting, online voting, e-voting, i-voting e-governance, authentication, challenges, Gujarat, India

I. INTRODUCTION

India is the world's largest democracy with a population of over 1.21 billion. Of the various fundamental rights that the Indian constitution grants a citizen of this country, the right to vote to elect its own government at every level, lies at the heart of the democratic republic. Today, Internet is changing the entire perspective of delivery of quintessential services to citizens. With almost every sector adopting online means to service people better and e-governance taking a solid shape in running the country efficiently, it seems very logical to see e-voting/online voting as the next step. As a matter of fact, a successful attempt at a small scale has already been initiated from the frontier of the state of Gujarat in India.

II. THE TRANSITION

Indian elections are based on the first-past-the-post system[1] with universal adult suffrage[2]. The first two general elections in 1952 and 1957 saw the simple *"balloting system"* as the foundation for the election process wherein at every polling station a separate ballot box was placed for each candidate. This was followed by the *"Marking system"* of voting in which the elector marked a ballot paper consisting of names of all contesting candidates and their election symbols and dropped in a common ballot box. The general elections of *Lok Sabha* in 2004 saw the full fledged use of the *"Electronic Voting Machines"* for elections that drastically eased the cumbersome process.

Internet voting has not yet been reliably accepted as the secure way to maintain the security, transparency, integrity and sanctity of an election. Several concerns have been raised time and again by security experts questioning internet as a suitable platform. Despite this, several nations, notably Estonia at national level and local governments of Canada at smaller level have managed to employ means to give a tangible shape to the idea with quite a success. Indian states have already started looking at the future prospect of implementing online voting, with the initial step already been taken by the state of Gujarat in 2011.

III. DEFINING THE TERM: INTERNET VOTING

Internet voting in generalized terms is the process of casting vote online via an online web portal over the internet using devices such as personal computer, laptop or mobile devices such as tablets and smart phones. The entire election process is dematerialized and everything is conceived and conducted over the virtual world via internet.

Internet voting can be conducted on site as well as remotely. On-site presents the ease of controlled settings such as kiosks or booths where authentication can be officially confirmed and voting can be done in secrecy. Remote internet voting on the other hand maximizes the convenience of the voter by letting the process to be conducted at their desired place of access (e.g. home/office computer, public library etc.)

[1] The first-past-the-post system, also called the simple plurality voting or single choice voting system is a single winner voting system where candidate securing the highest number of votes of a given electorate is the winner.

[2] Universal Adult suffrage implies providing the right to vote to adult citizens.

IV. ADVANTAGES OF INTERNET VOTING

The right to vote is the essence of a true democracy. Internet voting or e-voting has a paramount effect on increased civil participation. It becomes an incentive to young people who are up to date with the comfort and convenience of internet technologies. Keeping up with the recent trends is a way to promise democracy a chance to be bigger and better.

Internet voting promises *convenience, ease of accessibility, cost savings, fewer errors* and most intuitively an easier way to manage the counting of votes. The idea is a revolution in itself. It primarily aims at the section of the population that has a high internet usage and is technologically sound to use it. However it does come with some hurdles owing to the technological limitations. The risks fundamentally stand to challenge the electoral integrity-the very basic promise of a democracy. Maintaining transparency and the confidence of the public in the election, reliability of the process, and the authenticity of the citizen alongside the total anonymity of the same is a challenge in today's era of penetrating technologies.

V. CHALLENGES WITH INTERNET VOTING

The idea of internet voting revolves around the uncontrolled environment of Internet. This presents a set of risks and challenges, the most prominent of which are discussed further. (Fig. 1)

Security
Integrity
Unicity
Availability
Authentication
Anonymity
Secrecy
Transparency
Reliability
Auditablity

Fig. 1. Challenges with Internet Voting

A. *Security*

An online system of facilitating elections has its own sets of security vulnerabilities owing to the openness of the network. Untamed attacks and hacking threats with malicious intent are a serious issue when it comes to maintaining the integrity of the election process.

B. *Integrity*

Elections instill an abiding faith in the public of a democratic nation. It is of crucial importance to ensure the process of voting remains unhampered with and completes successfully and accurately.

C. *Unicity*

This refers to the *'one elector, one vote'* principle. Every person of voting age (and not deprived of his civil rights) can cast *one and only one vote*. Internet voting must be able to maintain this universal rule and ensure that in case multiple options for voting are allowed, only one vote against one elector is accepted.

D. *Availability*

The election process can be accorded limited flexibility with respect to time. The availability criterion[3] is hence very significant. The internet platform however can cause service disruptions due to a variety of reasons[4].

E. *Anonymity & Authentication*

The process of electoral voting demands a unique criterion of authentication and anonymity of the elector/voter. The process has to confirm whether a person is eligible to vote by authenticating the identity followed by a permanent dissociation of the process of casting of vote from the voter's identity to ensure anonymity. This is a challenge in itself.

Further the process requires guarding against impersonation or in between attacks. Implications in accessing the authenticated system also need to be carefully dealt with.

F. *Secrecy*

Until now, secrecy of ballots has been provided by allowing the process to be governed by a controlled environment in the presence of official authorities. However internet voting, especially remote internet voting cannot guarantee this advantage. Coercion is a known issue and internet voting as of now, fails in this regard.

For the virtual environment, maintaining secrecy is a challenge because of the need to maintaining authentication and anonymity at the same time while ensuring the integrity of process and its management.

G. *Transparency*

The credibility and integrity of the election process is directly associated with transparency. This opposes the common methodology employed in online transactions that directs towards *"security through obscurity"*. Public confidence is instilled with the fact that the entire process remains transparent; the casting and counting of vote must be open to public scrutiny. However technology by default obscures the counting process which reduces transparency to the minimum. Only processes that reflect the activity of

[3] The availability criterion refers to the state of online service being available throughout the determined time duration.

[4] For example, denial of service (*DoS*) attacks, phishing attacks, software issues, hardware malfunctioning, power outage and network disruptions.

the system can be monitored, which as very well may be distorted or misleading.

H. Reliability

The risks and vulnerabilities that arise in an online process for conducting elections are very hard to manage since everything becomes intangible. The entities[5] that can be checked, managed and controlled are all dematerialized into digital entities. The observations made via physical senses no longer apply. What cannot be seen cannot be scrutinized essentially. The entire process is invisible to the majority. Reliability of the election process is challenged to the core since not a single step in the process can be completely relied upon. Fraudulent code can change all the votes in one go and there would be no way of confirming that; a small number can only be needed to invalidate everything and with no expensive cost attached to it; and at the very least, there can be an unpredictable number of malfunctions either on the remote device, the network or the remote server itself.

I. *Auditability*

The fact that the process of election requires dissociation of identity of the voter from the vote cast makes it impossible to audit the process. The trail cannot be maintained if it has to be deleted. Further if any evidence of tampering with the process comes to light, there is no way to get back to the "previous" state.

This is contradictory to the voting secrecy and voter anonymity requirements. The entire election process getting virtualized in internet voting forces this contradiction as a result of which this challenge cannot possibly be managed.

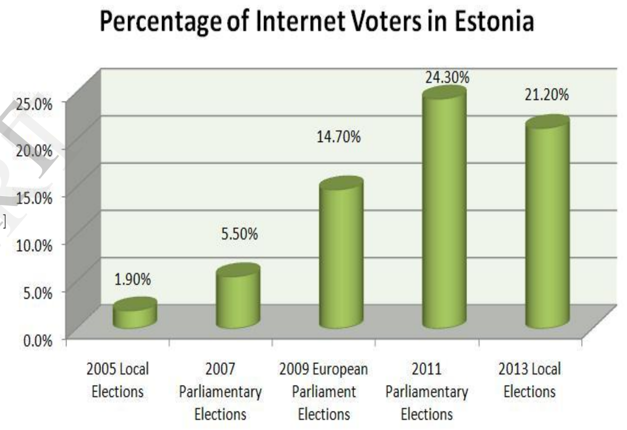
VI. GLOBAL EFFORTS TOWARDS INTERNET VOTING

Several countries have considered outweighing the advantages over the risks discussed in the previous section by mitigating them with preventive measures and deployed the methodology in public elections, either nationwide or at the small scale, preferably as an additional way to cast vote over the already existing processes. A few noteworthy implementations are discussed further.

Many European countries have trialed the online voting including Estonia, Switzerland, France, Germany, Spain, the Netherlands, and the United Kingdom.

Geneva, Switzerland has conducted the largest number of elections with Internet voting as an option for voters of any jurisdiction in the world [1]. Provided as an option along with in-person and postal voting, internet voting is implemented by allowing voters to access an e-Government service portal using a code printed on a voting card sent to them by post and casting their vote. Part of the code is kept secret under a scratch away layer. Voters are needed to provide shared secret information (date of birth and municipality of origin) to authenticate their identity online to the election server.

Estonia was the first nation to implement online voting for all voters at a national or supranational level of government. Internet voting was first introduced in the local elections of 2005 using smart cards, when more than 9 thousand voters cast their ballot via the Internet (this corresponded to about 2 per cent of all participating voters). Today, I-voting with binding results has been carried out *six times* in Estonia: in the local elections in October 2005, the parliamentary elections in March 2007, the European Parliament elections in June 2009, the local elections in October 2009, the parliamentary elections in March 2011 and the local elections in October 2013. In the 2011 parliamentary elections, almost a quarter of votes cast were Internet votes (Fig. 2)[6].



The 2011 elections to the Riigikogu also saw the use of mobile phones to cast I-votes. In 2012 a separate Electronic Voting Committee was established who is now responsible for conducting Internet voting while the National Election Committee retains a supervisory role.

Fig. 2. Percentage of Internet Voters in Estonia

Internet voting in Canada was first put to test in selected Ontario municipalities in 2003. Since then many municipalities have adopted the technology to reduce the tedious efforts required to conduct the intensive elections. As of 2011, six provinces have passed legislation allowing for various forms of electronic voting (Alberta, BC, New Brunswick, Nova Scotia, Ontario and Quebec), including Internet voting [2].

Internet voting efforts in USA saw a promising rise in early 2004 followed by a setback. There were small trials

[5] Entities such as ballots, ballot box, authentication proofs and signing sheets

[6] Official Statistics from http://vvk.ee

before, however the event in 2004 was significant. In 2002, The Federal Voting Assistance Program (FVAP), an agency within the Department of Defense began work on the Secure Electronic Registration and Voting Experiment (SERVE) [3]. Fifty-five counties from seven states viz. Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah and Washington, volunteered to participate [4]. According to the EAC report on SERVE, "services for voters included: online voter registration and updating of voter information online; ballot delivery and vote selection; and review of their registration and voting status."[5]. The SERVE technology was ready to conduct the first large scale multi-state online voting in an actual US election by the end of 2003. However the SERVE Security Peer Review Group (SPRG) in January 2004 raised serious concerns over security and eventually the project was put to halt. USA has been cautiously moving in this regard since then. In 2010, 33 states were using Internet voting to support military and overseas voting [6].

VII. SCRUTINY OF THE ATTEMPT OF INTERNET VOTING IN INDIA

India has been using electronic voting machines for over a decade now for the nationwide election process. However the nation is slowly and carefully attempting to achieve online authentication for all the citizens that holds a future prospect for implementing national level online voting. India's Unique Identification Authority *(UIDAI)* has laid the foundation for online authentication for government services by issuing a unique *Aadhar* card that provides with unique identification numbers to all Indian citizens along with linking biometric details of individuals. The issuing process is still undergoing and plans to issue 600 million numbers through its network of registrar offices located throughout the country by 2015[9].

The State of Gujarat made the first attempt to transition to Internet voting in September 2010 and the system was used again in municipal elections held in April 2011. The solution used by the State of Gujarat is developed by *Scytl*, a well-established Internet voting solution provider based in Spain [7]. This initiative called the *On-line Voting System* (OVS) was conceptualized in December 2009 and implemented in 6 municipal corporations, at the rate of one ward in each corporation, in 2010 and also in all the 11 wards in Gandhi Nagar Municipal Corporation, in 2011. In the April 2011 election, 77.16 percent of registered voters cast their votes online, either from their home computers, or from kiosks [7]. This initiative was conferred *Bronze award* in the category of "*Excellence in Government Process Re-engineering*" in the National e-Governance Awards, 2013.

A. *The Process*

The voting envisaged two options:

1. **1.** From Residence, or
2. **2.** From e-Polling booth

The citizen was required *to register* himself online at http://www.onlinevotinggujarat.gov.in giving his/her essential details including a valid email address and a mobile number. This was followed by physical verification of the e-voter's identity by a visit by authorized personnel to his/her residence verifying the details. Once the voter's identity was authenticated, he/she was recognized as an e-voter and a set of credentials was sent to the registered mobile to *activate the voting account*. The process was then materialized on the voting day when the e-voter could cast his/her vote by logging in on http://www.onlinevotinggujarat.gov.in, selecting a candidate from the digital ballot (with the option of changing the vote multiple times before submission) and then confirming the vote cast by entering a pass code sent via OTP[7] to the registered mobile. An encrypted receipt of successfully cast vote was then made available for print.

B. *Implementation Strategy*

State Election Commission (SEC), Gujarat attempted to envision computerization of all key processes in a local body election ensuring that the implemented system abides by the election process protocol. The online voting system (OVS) was laid as an additional option to voters to register as e-voters and cast their vote online remotely. Tata Consultancy Services (TCS) was selected as system integrator for developing the application.

The implementation team focused on:

1. Ensuring completeness and adherence to voting protocol as applicable to internet based voting.
2. Ensuring availability and reliability of the voting system.
3. Protection against DoS, hacking and phishing and intrusion attacks.
4. Ensuring authenticity of voter, here the voting client.
5. Ensuring authenticity of vote cast & digital non traceability of cast votes.
6. Secrecy of votes.
7. Maintaining integrity of ballots against attacks to distort it.
8. Ensuring non duplication of ballots and votes.

Standard cryptographic solution was implemented to encrypt the votes. Availability was ensured by deploying the system at two sites-primary (DC) and disaster recovery (DR), configured 1:1. Multiple level of security implementations were adopted including firewall, IPS/IDS, Anti Virus and Secure Socket Layer (SSL) encryption at Data Centre and Data Recovery sites.

The remote site through which the e-voter cast his/her vote was subject to the restriction of using the same personal

[7] One Time Password

computer/laptop to cast the vote that was used while activating the account. Also the casting of vote is layered by a second level of authentication by using an OTP pass code that can only be resend thrice.

Protection against malicious attacks was ensured by a modest combination of 1+1 redundancy, network monitoring, SSL authentication, standard encryption and stringent firewall policies.

The portal was also given genuine identification by security certification so that e-voters can be assured of the identity of the portal.

C. *Analysis*

Against the challenges discussed previously, the implementation attempt of Gujarat was reviewed as below:

1. *Challenge:* Security
   Mitigation Step(s): Network monitoring, Secure Socket Layer (SSL) authentication, standard encryption, stringent firewall policies, Intrusion Detection Systems, anti-virus scanning

   Remarks: Modest attempts for small scale implementation.

2. *Challenge:* Integrity
   Mitigation Step(s): Encryption of cast vote over network, providing security certificate of portal to recognize it, Encrypted receipt

   Remarks: Modest attempts for small scale implementation. However data still vulnerable to high end security attacks in the middle. Also vulnerabilities due to a falsified security certificate already installed on the device not put under consideration.

3. *Challenge:* Unicity
   Mitigation Step(s): Allowing changing of vote cast only before submission, either or option selection while registration by citizen

   Remarks: Achieved.

4. *Challenge:* Availability
   Mitigation Step(s): 1+1 redundancy by maintaining a DR site to the primary site for portal traffic and processing, large quantity of bandwidth

   Remarks: Modest approach restricted by common parameters such as common power grid or network cables.

5. *Challenge:* Authentication
Mitigation Step(s): Initial verification of voter's identity by personnel visits, Credentials for voting account, SSL encryptions, OTP pass code requirement for final submission of the vote

   Remarks: Impersonation has not been considered in case the credentials and the mobile is used by another person. Also vote-buying and coercion cases not considered.

6. *Challenge:* Anonymity
   Mitigation Step(s): Dissociation of encrypted vote as soon as the casting is done and received at the server

   Remarks: The vote cast can be attacked before dissociation and manipulated by attacks such as "man-in-the-middle"[8] despite SSL connections due to ever trending increase in programming capabilities that can be employed by hacking entities.

7. *Challenge*: Secrecy
   Mitigation Step(s): The entire process after casting under supervision of authenticated officials at server locations, Secure Socket Layer (SSL) Encryption, Voter Identity/Ballot Data Separation, and Voter Ballot Data Verification

   Remarks: Modest mitigation steps undertaken. Digital signatures could also have been used. Smart cards along with digital signatures also seem to be a good option as implemented in Estonia.

   The secrecy during casting is almost impossible on the remote site without trusting the e-voter.

8. *Challenge:* Transparency
   Mitigation Step(s): None.

   Remarks: Transparency hasn't been considered as such, since security measures overlap.

9. *Challenge:* Reliability
   Mitigation Step(s): Unknown

   Remarks: Several vulnerabilities as discussed previously.

10. *Challenge:* Auditability
    Mitigation Step(s): None

    Remarks: This fundamentally clashes with the requirement of anonymity. An attempt to maintain a log will inherently breach the voting secrecy.

Altogether the attempt was a humble start and stands to a promising improvement. Security, reliability and auditability concerns are prime concerns while authentication regime needs to be expanded. Further, as a

[8] Man in the middle attack is an active eavesdropping in which the attacker makes independent connections between source and destination entities and relays messages between them without the two recognizing that their conversation has been hacked.

scalability concern, availability is of concern too. Transparency is to be more intuitively dealt with, with better ways to turn the process as opaque to the citizens as possible. The initiative has a long way to go.

VIII. CONCLUSION

For an e-voting implementation to be acceptable, it must essentially meet a three-fold set of requirements viz. to be compliant to election legislation and principles, to be at least as secure and reliable as the regular voting process and to be as similar to the regular voting process as possible. As analyzed, internet voting presents multiple challenges at every level, from policy makers to code developers. The attempt of internet voting by the state of Gujarat is appreciable however still very premature when it comes to managing the crucial process of elections of the world's largest democracy. There are various promising advantages that this idea presents before us and the successes do depict that. Higher turnout, ease of accessibility, convenience in respect to in-person voting, better quality of service to citizens and easy management are motivational elements that are driving governments to attempt to implement internet voting at various scales. However this process entails with it several risks and compromises with a number of fundamental and universal principles associated with the election process. The invisibility and intangibility factor that arises from the virtualization, threatens risks of large scale frauds, and presents a compromise with transparency, reliability and the ability to audit the election process. Scalability in turn diversifies the issues exponentially. Nevertheless the idea needs to be nourished more in order to find the right set of implementation strategies. Continuously improving attempts can be sustained at small homogeneous level as advancements emerge and better options are made available.

REFERENCES

1. R. M. Alvarez, T.E. Hall, & A.H. Trechsel, “Internet Voting in Comparative Perspective: The Case of Estonia. PS: Political Science and Politics”, 2009, p. 497-505.
2. P. Laronde, “Technologies in the Voting process: An Overview of Emerging Trends and Initiatives”, May 2012.
3. A. Regenscheid, N. Hastings, "A Threat Analysis on UOCAVA Voting Systems", 2008, p. 04
4. Election Assistance Commission, “A Survey of Internet Voting”, September 2011, p. 29.
5. Election Assistance Commission, “A Survey of Internet Voting”, September 2011, p. 30.
6. Barnes, E., “Internet Voting Arrives...But is it Secret and Secure”, 2010.
7. Verified Voting, “Internet Voting in India? Gujarat is the Early Adopter”, May 2011.
8. Alootechie, “Gandhinagar Municipal Corporation uses internet voting technology for conducting elections”, May 2011.
9. M. Kripp, “Internet voting in Estonia - Internet voting is necessary to maintain turnout and integrate voters”, 2011
10. http://uidai.gov.in
11. http://vvk.ee
12. http://sec.gujarat.gov.in/e-voting-system.htm
13. http://sec.gujarat.gov.in/
14. http://eci.nic.in
15. http://en.wikipedia.org/wiki/Electronic_voting